UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TENNESSEE

NATIONAL BOARD OF MEDICAL EXAMINERS *et al.*,	)	
Plaintiffs,	)	
v.	)	**Civil Action No. 09-1043-JDB**
OPTIMA UNIVERSITY LLC *et al.*,	)	
Defendants.	)	

DECLARATION OF KEN G. TISDEL

I, Ken G. Tisdel, hereby state as follows:

1. My name is Ken G. Tisdel. I am more than twenty-one (21) years of age and, unless otherwise noted, I have personal knowledge of the facts stated herein.

2. I am the President and Co-Principal for Lateral Consulting Group LLC., in Houston, Texas, and I have been with this company since its inception in October 2008.

3. I have over nine years of experience in the field of computer forensic investigations. Prior to my position as the President for Lateral Consulting Group, I was a Director with Huron Consulting Group where I ran the operations of the Houston, Texas computer forensics practice that I helped to build. I also was employed for over nine years as a Certified Law Enforcement Officer in both Arizona and Vermont.

4. During the last six years of my law enforcement tenure, I was assigned to the Internet Crimes Against Children Task Force (ICAC) and the Vermont Internet Crimes Task Force (VTICTF), working directly with the Federal Bureau of Investigation,

United States Secret Service and the Department of Homeland Security, investigating computer and internet based crimes. Since my move to civil litigation, I have performed and managed hundreds of complex computer forensic investigations and provided expert opinion and testimony on a broad range of matters including FCPA investigations, SEC and DOJ investigations, employment agreement violations and trade secret misappropriations.

5. I have provided sworn testimony in over 30 separate criminal and civil matters and have been recognized as a computer forensics expert by courts in Texas, West Virginia, Vermont and Connecticut. I frequently provide training to other computer forensic examiners on the methods and procedures related to expert testimony.

6. Lateral Consulting Group LLC. (LCG) was retained by the National Board of Medical Examiners and the Federation of State Medical Boards and their attorneys to provide technical assistance and consultation regarding the collection and preservation of electronic data in connection with the above-captioned lawsuit involving Optima University.

7. On February 24, 2009, two analysts from LCG traveled to Optima University's facilities near Jackson, Tennessee to forensically capture/image relevant electronic data storage devices that were found on-site. Multiple computers were located on-site and several images were gathered by LCG's analysts. At some point during the visit, the owner of Optima arrived and was introduced to our analysts as a Dr. Suliman.

8. Our analysts attempted to capture an image of Dr. Suliman's laptop computer during this initial visit. However, it was found to be encrypted and Dr.

Suliman was unwilling to provide the encryption password(s). Many computers were being utilized in multiple computer "class rooms" at the Optima site, and they appeared to be networked to a server. I have been informed that Dr. Suliman told our analysts that there were no servers on site and that the computers were networked to a server in Romania.

9. This turned out to be untrue. With assistance from two Agents with two U.S. Marshals, our analysts located a room in the lower level that contained 3 servers.

10. Because of the lack of cooperation that our analysts received during the initial visit to Optima, we had to make a second trip to Optima's facilities to once again attempt to collect and image the computers that were not imaged on the previous trip. We did so on March 26, 2009, after the plaintiffs' attorneys had arranged for a second visit with the defendants' attorneys. It is my understanding that Dr. Suliman and his attorney advised that LCG would receive complete cooperation during this visit and that all passwords and access to all computers would be provided. I participated in the second visit, along with LCG analyst Alex Fredette. We were accompanied by one of the plaintiffs' attorneys and a U.S. Marshal. At Optima, we met with Dr. Suliman and with a computer technician who Dr. Suliman or his attorney had apparently retained to assist on this matter, James Reed.

11. Upon initial review of Dr. Suliman's Sony VAIO laptop, Mr. Fredette observed that the laptop had been encrypted with TrueCrypt disk encryption software. Mr. Fredette found that there were two hard drives installed in the laptop, a 250gb drive and a 200gb drive – both drives were encrypted. Mr. Fredette also located over 300gb of free space on the laptop that was contained within two partitions. Finding free space

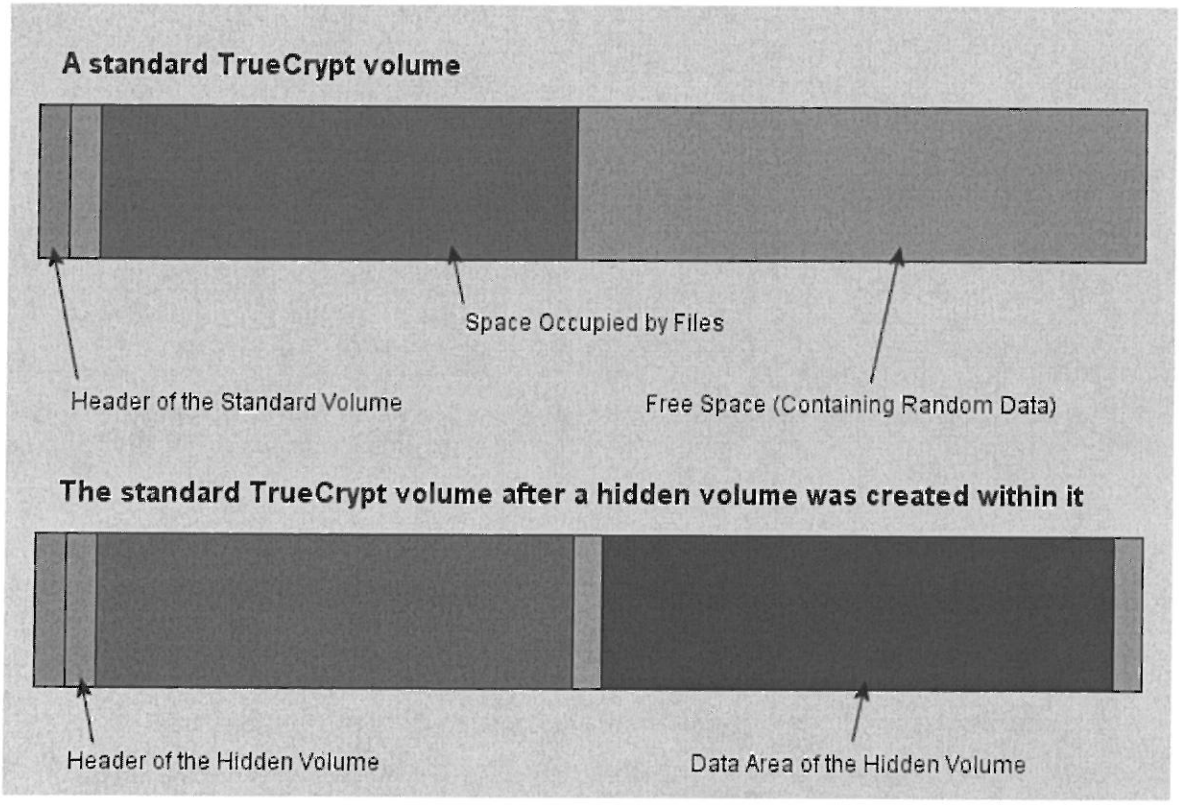
within two separate volumes, especially of this size (over 300gb), is almost unheard of. Considering the configuration of the computer having two hard drives and both of them being under 300gb each, I was quite surprised to not find one bit of data contained within these volumes. From looking further we found that on the 200gb drive there was approximately 70gb of data which consisted of the Windows Operating System, Installed Software, and few links to bankruptcy sites and other miscellaneous web hits. Beyond that 70gb of data there was no other visible data on the computer.

12. Upon locating this free space, I asked Dr. Suliman how long he had owned the laptop. Dr. Suliman stated that he had owned the laptop for a long time "since 1999". I immediately knew that this statement was false since the laptop had a port for HDMI, which was not being installed into computers until approximately 1 to 2 years ago.

13. I asked Dr. Suliman if he had recently deleted any large amounts of data from his laptop, because our identification of the 300gb of free space over two volumes was extremely suspicious and rarely seen in computers that were used frequently. Dr. Suliman stated that he hardly ever used the computer. This statement also appeared to be false, due to the physical appearance of the computer showing signs of wear and frequent use (shiny spots on the keys from friction wear, dirt build up, etc...).

14. TrueCrypt advertises a feature that will allow a user to encrypt and hide volumes on a hard drive. TrueCrypt states the following on their website:

> **Hidden Volume**
>
> It may happen that you are forced by somebody to reveal the password to an encrypted volume. There are many situations where you cannot refuse to reveal the password (for example, due to extortion). Using a so-called hidden volume allows you to solve such situations without revealing the password to your volume.



The layout of a standard TrueCrypt volume before and after a hidden volume was created within it.

The principle is that a TrueCrypt volume is created within another TrueCrypt volume (within the free space on the volume). Even when the outer volume is mounted, it is impossible to prove whether there is a hidden volume within it or not*, because free space on *any* TrueCrypt volume is always filled with random data when the volume is created** and no part of the (dismounted) hidden volume can be distinguished from random data. Note that TrueCrypt does not modify the file system (information about free space, etc.) within the outer volume in any way.

The password for the hidden volume must be substantially different from the password for the outer volume. To the outer volume, (before creating the hidden volume within it) you should copy some sensitive-looking files that you actually do NOT want to hide. These files will be there for anyone who would force you to hand over the password. You will reveal only the password for the outer volume, not for the hidden one. Files that really are sensitive will be stored on the hidden volume.

A hidden volume can be mounted the same way as a standard TrueCrypt volume: Click *Select File* or *Select Device* to select the outer/host volume (important: make sure the volume is *not* mounted). Then click *Mount*, and enter the password for the hidden volume. Whether the hidden or the outer volume will be mounted is determined by the entered password (i.e., when you enter the password for the outer volume, then the outer volume will be mounted; when you enter the password for the hidden volume, the hidden volume will be mounted).

TrueCrypt first attempts to decrypt the standard volume header using the entered password. If it fails, it loads the area of the volume where a hidden volume header can be stored (i.e. the bytes 65536–131071, which contain solely random data when there is no hidden volume within the

volume) to RAM and attempts to decrypt it using the entered password. Note that hidden volume headers cannot be identified, as they appear to consist entirely of random data. If the header is successfully decrypted (for information on how TrueCrypt determines that it was successfully decrypted, see the section Encryption Scheme), the information about the size of the hidden volume is retrieved from the decrypted header (which is still stored in RAM), and the hidden volume is mounted (its size also determines its offset).

A hidden volume can be created within any type of TrueCrypt volume, i.e., within a file-hosted volume or partition/device-hosted volume (requires administrator privileges). To create a hidden TrueCrypt volume, click on *Create Volume* in the main program window and select *Create a hidden TrueCrypt volume*. The Wizard will provide help and all information necessary to successfully create a hidden TrueCrypt volume.

When creating a hidden volume, it may be very difficult or even impossible for an inexperienced user to set the size of the hidden volume such that the hidden volume does not overwrite data on the outer volume. Therefore, the Volume Creation Wizard automatically scans the cluster bitmap of the outer volume (before the hidden volume is created within it) and determines the maximum possible size of the hidden volume.***

If there are any problems when creating a hidden volume, refer to the chapter Troubleshooting for possible solutions.

Note that it is also possible to create and boot an operating system residing in a hidden volume (see the section Hidden Operating System).

* Provided that all the instructions in the TrueCrypt Volume Creation Wizard have been followed and provided that the precautions mentioned in the subsection Security Precautions Pertaining to Hidden Volumes are followed.

** Provided that the options *Quick Format* and *Dynamic* are disabled and provided that the volume does not contain a filesystem that has been encrypted in place (TrueCrypt does not allow the user to create a hidden volume within such a volume). For information on the method used to fill free volume space with random data, see chapter Technical Details, section TrueCrypt Volume Format Specification.

*** The wizard scans the cluster bitmap to determine the size of the uninterrupted area of free space (if there is any) whose end is aligned with the end of the outer volume. This area accommodates the hidden volume and therefore the size of this area limits the maximum possible size of the hidden volume. On Linux and Mac OS X, the wizard actually does not scan the cluster bitmap, but the driver detects any data written to the outer volume and uses their position as previously described.

15. I asked Dr. Suliman if he had utilized the "Hidden Volume" feature provided within the TrueCrypt software. Dr. Suliman said that he did not know what I was talking about. He stated that he did not know anything about computers and that the only thing he knew how to do with a computer was how to turn it on and off.

16. I questioned him about his statement since the use of TrueCrypt and the setup of his laptop significantly exceeded the abilities of someone who only knew how

to turn a computer on and off. Dr. Suliman again stated that he only knew how to turn it on and off and that he had nothing to do with the set up of the laptop and that everything I was talking about was foreign to him.

17. We asked if he had any additional passwords that he used on the laptop and he was adamant that he had already provided us with the only passwords used and that there weren't any additional passwords. It should be noted that Dr. Suliman's choice of passwords were some of the most complex passwords that I have seen in my career. The passwords used were as follows:

atrialseptaldefect

thelper1cellmediatedimmunity

patentforamenovale

18. Dr. Suliman recommended that I speak with someone who he identified as his IT administrator in Romania and said that he could possibly answer any questions that I might have. Dr. Suliman made a call from his cell phone and told his IT administrator to assist me. Dr. Suliman handed me the phone and told me that I would be speaking with Adrian Praja. I spoke with Adrian for several minutes about the laptop configuration. Adrian advised that he didn't have much knowledge about the setup of Dr. Suliman's laptop, nor was he familiar with the configuration of TrueCrypt and Dr. Suliman's use of it.

19. I asked Adrian how he handled the backups for the server environment. Adrian asked what I meant and I explained that I wanted him to describe what activities he would perform if all of the servers at Optima University were to crash and completely lose all data. Adrian said that he would reinstall all the software remotely

from Romania. I asked him how he would reinstall all of the test questions. Adrian stated that he would load them via Microsoft Word documents. I asked him if he had those documents with him in Romania and he said that he did. I asked him if he could send me all of the test question Word documents via email. Adrian asked if he was allowed to and I told him that we had been informed that Dr. Suliman and Optima University would cooperate fully and that the test questions were what we were attempting to obtain.

20. Adrian took my email address from me and proceeded to send me 7 emails with large .zip files containing many Word documents of what appeared to be multiple choice medical test questions.

21. We then attempted to image Dr. Suliman's laptop via a live capture due to the use of encryption software. The first two images failed from "Delayed Write Failures" – the cause of this failure is unknown. A third attempt was successful but slow due to the live image being pulled through the USB port (over 8 hours to image the 200gb drive). A request was made to take the laptop back to LCG labs in Houston to complete the image of the second 250gb drive due to an estimate that the image would take over 12 hours to complete. Dr. Suliman agreed to allow us to take the laptop and complete the imaging. (Dr. Suliman later changed his mind and didn't want the laptop to leave – he had a lengthy conversation with his brother and eventually gave us permission to take it.)

22. Dr. Suliman also had a 1TB USB external hard drive which we believe might contain relevant data. Dr. Suliman agreed that we could take the drive back to

our lab to complete the imaging due to the amount of time that would be required to image a drive of that size.

23. We also attempted to obtain an image from several of the desktop computers in the class rooms. Each image attempt was unsuccessful. None of our forensic tools were able to view the drives once they were connected. The cause of this error is unknown and has never been encountered in my past experience, but I believe that the cause was due to a Terminal Services environment that utilized a server to run each computer terminal. Under this type of setup there would not have been any data stored on the individual hard drives.

24. During this trip we also attempted to image the servers that were not made available during the previous visit. One of the servers that was responsible for the network switch, and most likely would not have contained any relevant data, had a bad drive (indicated by an orange flashing light). When the server was rebooted for imaging it would not restart due to the bad drive. One other server was successfully imaged. This server was running "Free BSD" for the operating system. This image was later brought back to LCG labs for further analysis.

25. During the failed attempt to image the switch server with the bad drive, we observed that the server was searching for a Windows server when it was trying to boot up. There were no Windows based servers that could be located at this facility. Dr. Suliman advised that the Windows server was in Romania.

26. The laptop and USB drive belonging to Dr. Suliman were brought back to LCG where they were successfully imaged and returned to Dr. Suliman's attorney via FedEx overnight.

27. We performed a forensic analysis on the image of Dr. Suliman's laptop computer. The analysis showed that on the morning of March 26, 2009, at approximately 9:30 am, the data-wiping utility "Eraserl.exe" was run on Dr. Suliman's laptop. This was at or just prior to the time that we arrived at Optima for our second visit on March 26th. This specific wiping utility deletes the user specified data and overwrites the data with "WipeDrive ---www.gaijin.at---". Our forensics analysis also revealed that Dr. Suliman's laptop was connected to an FTP site from at least 3/25/09 and perhaps earlier. FTP sites are utilized as storage locations where an individual can move files from a computer to an FTP site (which can be an on-site or off-site server) and later retrieve the documents at a later date from any computer. Additional forensic analysis showed that on 3/11/09 the entire operating system on Dr. Suliman's laptop was completely reinstalled. This type of activity is performed when a user wants to get rid of data to prevent future retrieval of the data or when the user has so many problems with a computer that it crashes beyond repair and a reinstall is the only solution to get the computer running again (which I don't believe was the case since I asked doctor Suliman if he had any problems with the computer in the past – the panel covering the hard drives was missing – and Dr. Suliman stated that the computer has always worked just fine and that there have not been any problems with it). This reinstallation process would have extremely hampered, and could have prevented altogether, the ability to recover any data and to identify any activity that was present on the computer prior to the reinstallation.

28. The analysis of Dr. Suliman's laptop computer and external USB drive is ongoing. The statements made in this report are based on preliminary analysis and additional details related to our continued analysis will be forthcoming.

29. Based on the preliminary findings from our initial analysis, as well as my experience in this field of work for over a decade in both a law enforcement and civilian capacity, there is no question that specific activities were taken to hide, relocate and prevent the recovery and viewing of data that at one time resided or continues to reside (in an encrypted and hidden format) on Dr. Suliman's laptop computer or on an FTP site.

30. Dr. Suliman's assistance and cooperation during this second collection attempt was not what we had hoped for. Dr. Suliman was elusive about our questions and at times his responses were outright deceptive as he would contradict himself with his responses to other questions. Dr. Suliman claimed that no one had removed or replaced any hard drives in any of the computers in the classrooms. However, of the computers that we opened, we found that the inside of the computer was covered in a layer of dust and yet the hard drive was perfectly clean (some drives had the word "clone" written on them with permanent ink). Clean drives typically indicate that someone has recently removed the drive and/or replaced it with another drive – otherwise the drive would be just as dirty as the rest of the interior of the computer. Dr. Suliman denied any knowledge of such activity.

31. When Dr. Suliman was asked for the password to the classroom computers, he stated that it was "optimapc". We made multiple attempts to access the computers with this password and had no luck. He continually told us the password

was "optimapc" and that he didn't know what to tell us. I asked if there were capital letters used or numbers and he said, "No, just optimapc". Finally I asked Dr. Suliman to enter the password. He sat down and quickly typed in many more keystrokes than what was required for "optimapc". I asked him what he had just typed and he stated, "optimapc". I powered down the computer and told him to enter it again, slowly. This time he entered:

o
key to the right of o
p
key to the right of p
t
key to the right of t
i
key to the right of i

and so on. Thus, the password was not actually "optimapc", it was "opp[tyiom,asp[cv".

32. I explained the issues that we were seeing with his laptop and the other computers in every way possible to make sure that there wasn't a language barrier, but I am confident that Dr. Suliman was aware of what it was that we were looking for, that he had intentionally taken steps to hide or delete that data just prior to our arrival and that he was trying to cover up that fact by claiming ignorance about computers and the network – even though his contradictory statements and the visible environment gave a different story.

33. Had Dr. Suliman truly cooperated with us and had he been truthful in answering our questions, this collection could have been completed in less than 5 hours, rather than the 14 hours that was spent on site and we still failed to walk away with the expected results.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on April 9th, 2009.

Ken G. Tisdel